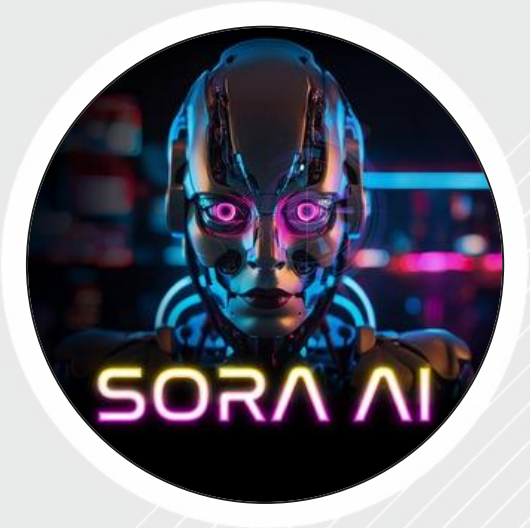
SPYWOLF

Security Audit Report



Audit prepared for

SORA AI

Completed on

February 25, 2024

KEY RESULTS

Cannot mint new tokens	Passed
Cannot pause trading (honeypot)	Passed
Cannot blacklist an address	Passed
Cannot raise taxes over 25%?	Passed
No proxy contract detected	Passed
Not required to enable trading	Passed
No hidden ownership	Passed
Cannot change the router	Passed
No cooldown feature found	Passed
Bot protection delay is lower than 5 blocks	Passed
Cannot set max tx amount below 0.05% of total supply	Passed
The contract cannot be self-destructed by owner	Passed

For a more detailed and thorough examination of the heightened risks, refer to the subsequent parts of the report.

N/A = Not applicable for this type of contract

*Only new deposits/reinvestments can be paused

OVERVIEW

This goal of this report is to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team’s evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

SORA AI

PROJECT DESCRIPTION

According to their website:
SORA is an AI model that can create realistic and imaginative scenes from text. SORA AI will start new era on blockchain technology.
SORA AI community is a place where token holders, enthusiasts, and the curious minds of the AI video creation world come together.

Release Date: Presale starts in February, 2024

Category: Meme token

CONTRACT INFO

Token Name
SORA AI

Symbol
SORA

Contract Address
0xC353Ca27ED7B6b7c361c4a86c3d562291734DE34

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Feb 24, 2024

Contract Type
Token with taxes

Total Supply
1,000,000,000

Status
Not launched

TAXES

Buy Tax
3%

Sell Tax
3%

*Taxes cannot be changed

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	1000000000 SORA
Median Transfer Amount	1000000000 SORA
Average Transfer Amount	1000000000 SORA
First transfer date	2024-02-24
Last transfer date	2024-02-24
Days token transferred	1

SMART CONTRACT STATS

Calls Count	2
External calls	2
Internal calls	0
Transactions count	2
Uniq Callers	1
Days contract called	1
Last transaction time	2024-02-24 10:20:23 UTC
Created	2024-02-24 10:18:53 UTC
Create TX	0x63c95e57962949dfa1ea0b751c9fdf26a93780f142646c168d8f8deb1dd48352
Creator	0xe314dfe43f47bf79a765313c3120048ab5717867

FEATURED WALLETS

Owner address	0xe314DfE43f47BF79A765313c3120048aB5717867
Marketing fee receiver	0x019d1280d3fc589AD19bB11C04Dd9e066D765284
LP address	0xc11f797d346d7F710e302715E354832c23527a50

TOP 3 UNLOCKED WALLETS

100%	0xe314DfE43f47BF79A765313c3120048aB5717867 (owner) *Tokens are not distributed yet*
N/A	
N/A	

VULNERABILITY ANALYSIS

ID	Title	
SWC-100	Function Default Visibility	**Passed**
SWC-101	Integer Overflow and Underflow	**Passed**
SWC-102	Outdated Compiler Version	**Passed**
SWC-103	Floating Pragma	**Passed**
SWC-104	Unchecked Call Return Value	**Passed**
SWC-105	Unprotected Ether Withdrawal	**Passed**
SWC-106	Unprotected SELFDESTRUCT Instruction	**Passed**
SWC-107	Reentrancy	**Passed**
SWC-108	State Variable Default Visibility	**Passed**
SWC-109	Uninitialized Storage Pointer	**Passed**
SWC-110	Assert Violation	**Passed**
SWC-111	Use of Deprecated Solidity Functions	**Passed**
SWC-112	Delegatecall to Untrusted Callee	**Passed**
SWC-113	DoS with Failed Call	**Passed**
SWC-114	Transaction Order Dependence	**Passed**
SWC-115	Authorization through tx.origin	**Passed**
SWC-116	Block values as a proxy for time	**Passed**
SWC-117	Signature Malleability	**Passed**
SWC-118	Incorrect Constructor Name	**Passed**

VULNERABILITY ANALYSIS

ID	Title	
SWC-119	Shadowing State Variables	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed
SWC-122	Lack of Proper Signature Verification	Passed
SWC-123	Requirement Violation	Passed
SWC-124	Write to Arbitrary Storage Location	Passed
SWC-125	Incorrect Inheritance Order	Passed
SWC-126	Insufficient Gas Griefing	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed
SWC-128	DoS With Block Gas Limit	Passed
SWC-129	Typographical Error	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed
SWC-131	Presence of unused variables	Passed
SWC-132	Unexpected Ether balance	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed
SWC-134	Message call with hardcoded gas amount	Passed
SWC-135	Code With No Effects	Passed
SWC-136	Unencrypted Private Data On-Chain	Passed

VULNERABILITY ANALYSIS

NO ERRORS FOUND

MANUAL
CODE REVIEW

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time.

We categorize these vulnerabilities by 4 different threat levels.

THREAT LEVELS

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance, functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Medium Risk

Sending value with balance and call success checks.
In context of the current contract this may lead to undesired behaviour.
If contract's balance is not enough and/or sending value fails, contract will halt on sell.

```
function sendValue(address payable recipient, uint256 amount) internal {
    require(
        address(this).balance >= amount,
        "Address: insufficient balance"
    );

    (bool success, ) = recipient.call{value: amount}("");
    require(
        success,
        "Address: unable to send value, recipient may have reverted"
    );
}

function _transfer(
    address sender,
    address recipient,
    uint256 amount
) internal override {
.......................
if (providingLiquidity && sender != pair)
    Liquify(feeswap, currentTaxes);
.......................
}


function Liquify(uint256 feeswap, Taxes memory swapTaxes) private lockTheSwap {
.................
uint256 marketngtxwAmt = unitBalance * 2 * swapTaxes.marketngtxw;
if (marketngtxwAmt > 0) {
    payable(marketngtxwWallet).sendValue(marketngtxwAmt);
}

uint256 devAmt = unitBalance * 2 * swapTaxes.dev;
if (devAmt > 0) {
    payable(devWallet).sendValue(devAmt);
}
.................
}
```

- Recommendation:
  - Remove the require statements from sendValue() function.

FOUND THREATS

Informational

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function AddExemptFee(address _address) external onlyOwner {
    exemptFee[_address] = true;
}

function RemoveExemptFee(address _address) external onlyOwner {
    exemptFee[_address] = false;
}

function AddbulkExemptFee(address[] memory accounts) external onlyOwner {
    for (uint256 i = 0; i < accounts.length; i++) {
        exemptFee[accounts[i]] = true;
    }
}

function RemovebulkExemptFee(address[] memory accounts) external onlyOwner {
    for (uint256 i = 0; i < accounts.length; i++) {
        exemptFee[accounts[i]] = false;
    }
}
```

FOUND THREATS

Informational

Owner can withdraw any tokens from the contract, except the native SORA token.
When this function is present, in cases tokens and/or bnb are sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```
function rescueBNB(uint256 weiAmount) external onlyOwner {
    payable(owner()).transfer(weiAmount);
}

function rescueBEP20(address tokenAdd, uint256 amount) external onlyOwner {
    require(tokenAdd != address(this), "Owner can't claim contract's balance of its own tokens");
    IERC20(tokenAdd).transfer(owner(), amount);
}
```

Owner can enable trading only once.
Trading is currently enabled.

```
function EnableTrading() external onlyOwner {
    require(!tradingEnabled, "Cannot re-enable trading");
    tradingEnabled = true;
    providingLiquidity = true;
    genesis_block = block.number;
}
```

Enable trading tx:
https://bscscan.com/tx/0xf9aea99586006c75d9693a8250f220b0985aa44a7475c64466c0617cd3447715

There is no information about the initial tokens distribution based on the project's whitepaper and/or website.

TOKENOMICS

WEBSITE

Website URL
https://www.soraaireal.com/

Domain Registry
http:s//www.wix.com

Domain Expiration
2025-02-23

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

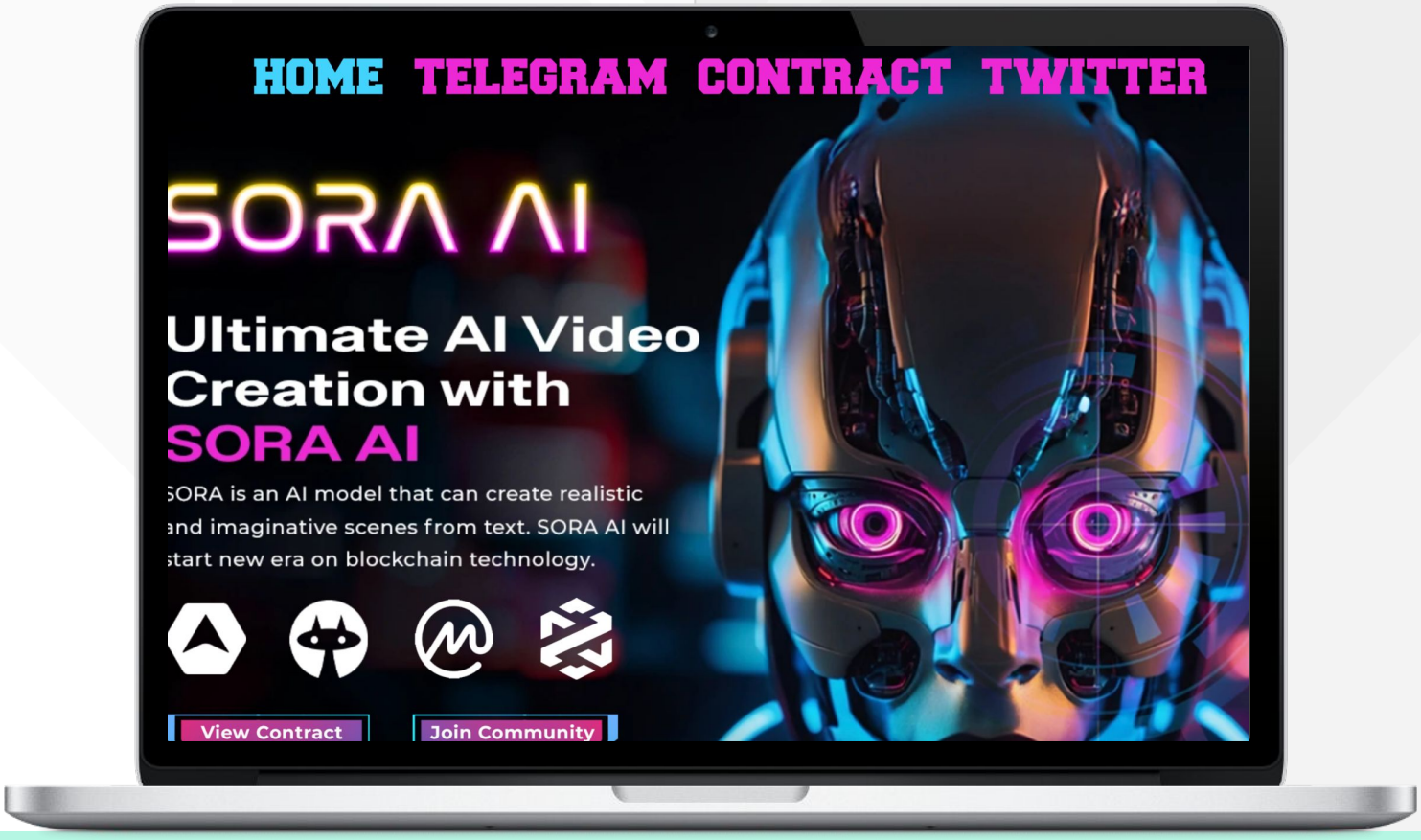
Design
Single page design with appropriate color scheme and graphics.

Content
Not very informative. No grammar errors found.

Whitepaper
No

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes



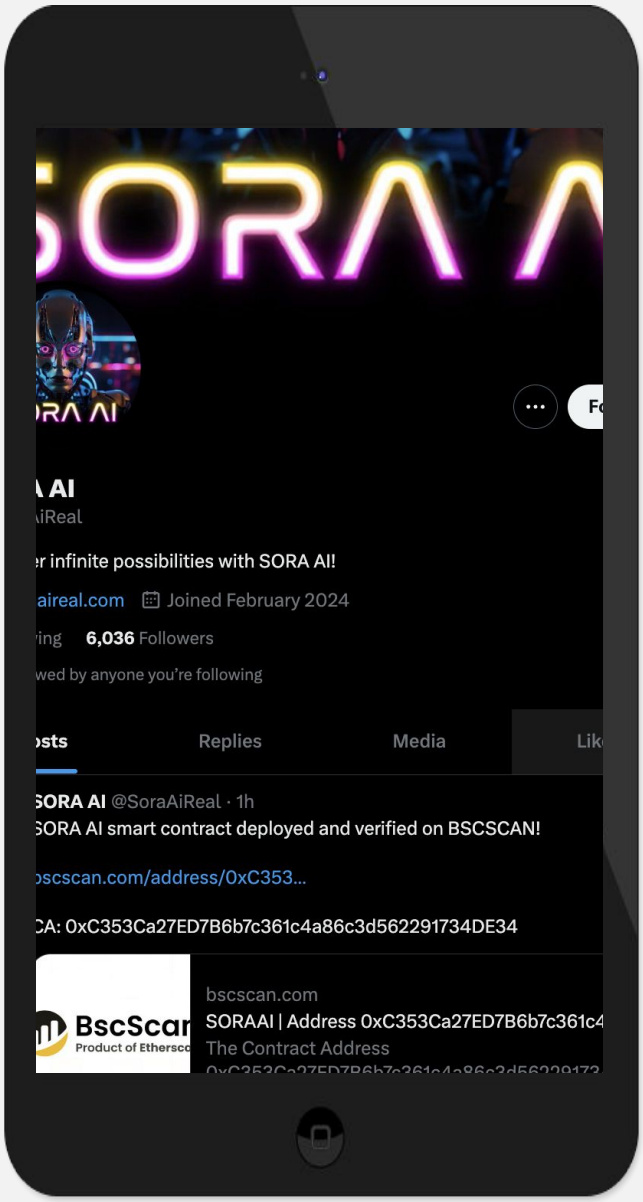
soraaireal.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active



Twitter's X

@SoraAiReal

- 6 193 followers
- Active
- Posts frequently

Discord

Discord link

- Not available

Telegram

@SoraAiREAL

- 4 667 members
- Active members
- Active mods

Medium

Medium link

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 700 SUCCESSFUL CLIENTS**
- **MORE THAN 1000 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.